UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND
Northern Division (Baltimore)

DALE FOSTER, DARLA SOLOMON, and DAVID LEITHREN, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

LOWER LLC,

Defendant.

Civil Action No. 1:22-CV-1581 (GLR)

JURY DEMAND

AMENDED CLASS ACTION COMPLAINT

Plaintiffs Dale Foster, Darla Solomon, and David Leithren ("Plaintiffs") bring this Complaint against Lower LLC ("Defendant" or "Lower"), in their individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. This class action arises out of the recent data breach ("Data Breach") involving Defendant, a domestic for-profit financial firm with locations around the United States.

2. Defendant failed to reasonably secure, monitor, and maintain Personally Identifiable Information ("PII") provided by consumers or companies that service consumers, including, without limitation, names, Social Security numbers, driver's license numbers, dates of birth, and financial account information, that it stored on its private network. As a result, Plaintiffs and other consumers suffered present injury and damages in the form of identity theft, loss of value of their PII, out-of-pocket expenses and the value of their time reasonably incurred to remedy or

mitigate the effects of the unauthorized access, exfiltration, and subsequent criminal misuse of their sensitive and highly personal information.

3. Moreover, after learning of the Data Breach, Defendant waited over six months (from December 14, 2021 to May 27, 2022) to notify Plaintiffs and Class Members of the Data Breach and/or inform them that their PII was compromised. During this time, Plaintiffs and Class Members were unaware that their sensitive PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

4. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant's conduct in breaching these duties amounts to negligence and/or recklessness and violates federal and state statutes.

5. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to take reasonable steps to protect the PII of Plaintiffs and Class Members and warn Plaintiffs and Class Members of Defendant's inadequate information security practices. Defendant disregarded the rights of Plaintiffs and Class Members by knowingly failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use.

6. As a direct and proximate result of Defendant's data security failures and the Data Breach, the PII of Plaintiffs and Class Members was compromised through disclosure to an

unknown and unauthorized third party, and Plaintiffs and Class Members have suffered actual, present, concrete injuries. These injuries include: (i) the current and imminent risk of fraud and identity theft (ii) lost or diminished value of PII ; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII; (vi) the invasion of privacy; (vii) the compromise, disclosure, theft, and unauthorized use of Plaintiffs and the Class Members' PII; and (viii) emotional distress, fear, anxiety, nuisance and annoyance related to the theft and compromise of their PII.

7. Plaintiffs and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and remains at risk due to inadequate data security.

8. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

Plaintiff Dale Foster

9. Plaintiff Dale Foster is, and at all times relevant has been, a resident and citizen of Columbia, Maryland, where he intends to remain. Plaintiff Foster received a "Notice of Data Incident" letter dated May 27, 2022, on or about that date.

10. The letter notified Plaintiff Foster that on December 14, 2021, Defendant discovered unusual activity in its systems and subsequently determined, on December 17, 2021, that an unauthorized person accessed Defendant's systems and exfiltrated consumers' data between December 10, 2021 and December 14, 2021. The letter further stated that Lower had also identified suspicious activity in its employee email accounts between September 2, 2021 and December 16, 2021. Lower also stated that it did not identify, until April 28, 2022, that consumers' names and social security numbers had been impacted by the Data Breach. Lower additionally noticed consumers that it maintained their drivers' license numbers, dates of birth, and financial account information and that such information was potentially impacted by the Data Breach as well.

11. The letter further advised Plaintiff Foster that he should spend time mitigating his losses by taking steps to help safeguard his information, including by following recommendations by the Federal Trade Commission regarding identity theft protection, resetting account passwords, contacting credit agencies, and placing a fraud alert or security freeze on his credit file.

12. The letter also encouraged Plaintiff Foster to sign up for one year of credit and identity monitoring through Experian IdentityWorks but simultaneously admonished him to self-monitor his credit for up to two years to detect fraud.

Plaintiff Darla Solomon

13. Plaintiff, Darla Solomon, is a natural person and citizen of Florida, currently residing in Port Saint Lucie, Florida. She intends to remain a citizen of Florida. She is a Data Breach victim who received Lower's breach notice August 2, 2022.

14. The letter notified Plaintiff Solomon that on December 14, 2021, Defendant discovered unusual activity in its systems and subsequently determined, on December 17, 2021,

that an unauthorized person accessed Defendant's systems and exfiltrated consumers' data between December 10, 2021 and December 14, 2021. The letter further stated that Lower had also identified suspicious activity in its employee email accounts between September 2, 2021 and December 16, 2021. Lower also stated that it "completed our more recent review effort" on July 7, 2022, and identified Plaintiff Solomon as a person whose data was impacted by the Data Breach.. Lower additionally noticed consumers that it maintained their drivers' license numbers, dates of birth, and financial account information and that such information was potentially impacted by the Data Breach as well.

15. The letter further advised Plaintiff Solomon that she should spend time mitigating her losses by taking steps to help safeguard her information, including by following recommendations by the Federal Trade Commission regarding identity theft protection, resetting account passwords, contacting credit agencies, and placing a fraud alert or security freeze on her credit file.

16. The letter also encouraged Plaintiff Solomon to sign up for one year of credit and identity monitoring through Experian IdentityWorks but simultaneously admonished her to self-monitor her credit for up to two years to detect fraud.

Plaintiff David Leithren

17. Plaintiff, David Leithren, is a natural person and citizen of Maryland, residing in Elkton, Maryland, where he intends to remain. He is a Data Breach victim who received Lower's breach notice in August of 2022.

18. The letter notified Plaintiff Leithren that on December 14, 2021, Defendant discovered unusual activity in its systems and subsequently determined, on December 17, 2021, that an unauthorized person accessed Defendant's systems and exfiltrated consumers' data

between December 10, 2021 and December 14, 2021. The letter further stated that Lower had also identified suspicious activity in its employee email accounts between September 2, 2021 and December 16, 2021. Lower also stated that it did not identify, until April 28, 2022, that consumers' names and social security numbers had been impacted by the Data Breach. Lower additionally noticed consumers that it maintained their drivers' license numbers, dates of birth, and financial account information and that such information was potentially impacted by the Data Breach as well.

19. The letter further advised Plaintiff Leithren that he should spend time mitigating his losses by taking steps to help safeguard his information, including by following recommendations by the Federal Trade Commission regarding identity theft protection, resetting account passwords, contacting credit agencies, and placing a fraud alert or security freeze on his credit file.

20. The letter also encouraged Plaintiff Leithren to sign up for one year of credit and identity monitoring through Experian IdentityWorks but simultaneously admonished him to self-monitor his credit for up to two years to detect fraud.

21. Defendant obtained and continues to maintain Plaintiffs' and Class Members' PII and has a continuing legal duty and obligation to protect that sensitive information from unauthorized access and disclosure. Plaintiffs would not have entrusted their PII to Defendant had they known that it would fail to maintain adequate data security. Plaintiffs' PII was compromised and disclosed as a result of the Data Breach.

Defendant Lower LLC

22. Defendant is a Maryland corporation with a principal office location of 8261 Robert Fulton Dr., Suite 150, Columbia, MD 21046.

23. Defendant is a broad-service financial firm and financial technology business, offering a wide range of loan services for individuals and businesses across the United States. Lower assists

consumers in finding the lowest rates for mortgage loans and insurance products through its website https://www.lower.com/finance (last accessed August 22, 2022) and the Lower smartphone application.

24. All of Plaintiffs' claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

25. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because many putative class members are citizens of a different state than Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

26. This Court has personal jurisdiction over Lower because it is headquartered in and maintains its principal place of business in this District. Lower is authorized to and regularly conducts business in Maryland. In this District, Lower makes decisions regarding corporate governance and management of its businesses, including decisions regarding the security measures to protect its customers' PII. Lower intentionally avails itself of this jurisdiction by promoting, selling and marketing its services from Maryland to thousands of consumers in Maryland and other states.

27. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because Lower's headquarters and principal place of business are located in this District, Lower resides in this District, and substantial parts of the events or omissions giving rise to the claims occurred in or emanated from this District, including, without limitation, decisions made by Lower's

governance and management personnel or inaction by those individuals that led to misrepresentations, invasions of privacy, and the Data Breach.

IV. FACTUAL ALLEGATIONS

Background

28. Defendant is a broad-service financial firm and financial technology business, offering a wide range of loan services for individuals and businesses across the United States. Lower assists consumers in finding the lowest rates for mortgage loans and insurance products through its website https://www.lower.com/finance (last accessed August 22, 2022) and the Lower smartphone application.

29. Plaintiffs and Class Members were persons who provided, or who third parties provided on their behalf, their PII to Defendant in conjunction with utilizing Defendant's mortgage and financial services.

30. Plaintiffs and Class Members relied on the sophistication of Defendant and its network to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII.

31. Defendant required the submission of and voluntarily accepted the PII as part of its business and had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumer's PII safe and confidential.

32. The information held by Defendant in its computer systems and networks (including its employee email accounts) included the unencrypted PII of Plaintiffs and Class Members.

33. Defendant retains and stores this information and derives a substantial economic benefit from the PII that it collects. But for the collection of Plaintiffs' and Class Members' PII, Defendant would be unable to perform its mortgage and financial services.

34. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

35. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

Defendant Lower Claims to Value Privacy and Security of PII

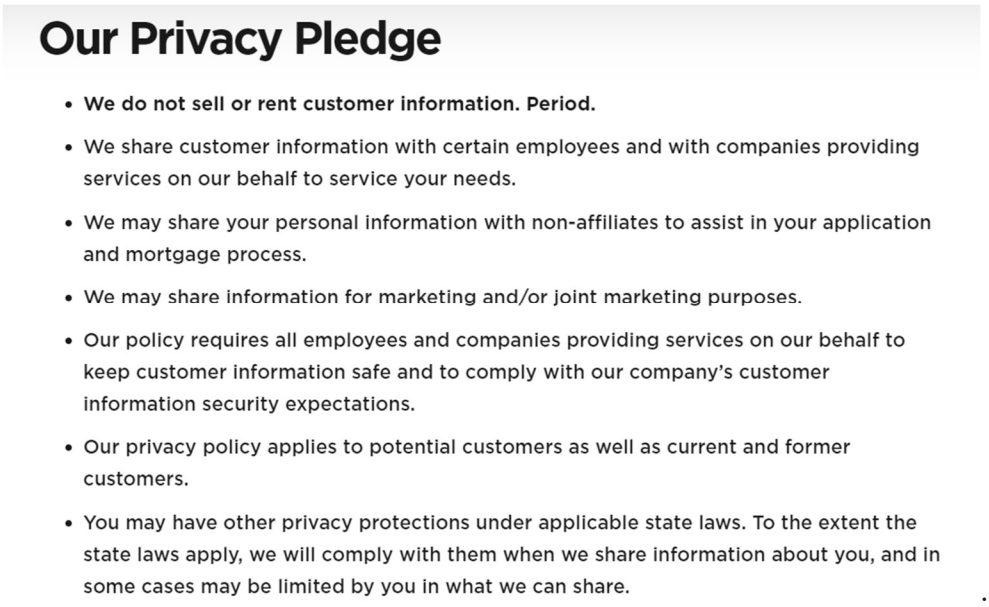
36. Defendant Lower's Privacy Policy[1] makes clear it believes in protecting confidential information:

> You are a valued customer and we at Lower, LLC ("Lower" or "Company") strongly believe in protecting the confidentiality and security of the information we collect about you as a customer, potential customer, or former customer. We have adopted the following policy to safeguard the personal information about you in our possession. Lower requires that its organization, employees, and its DBA/Other Trade Names, comply with all requirements of this policy.

37. Defendant Lower makes a bold privacy pledge[2] that it keep customer information safe:

[1] http://lower.com/legal/privacy-policy (last accessed August 22, 2022)

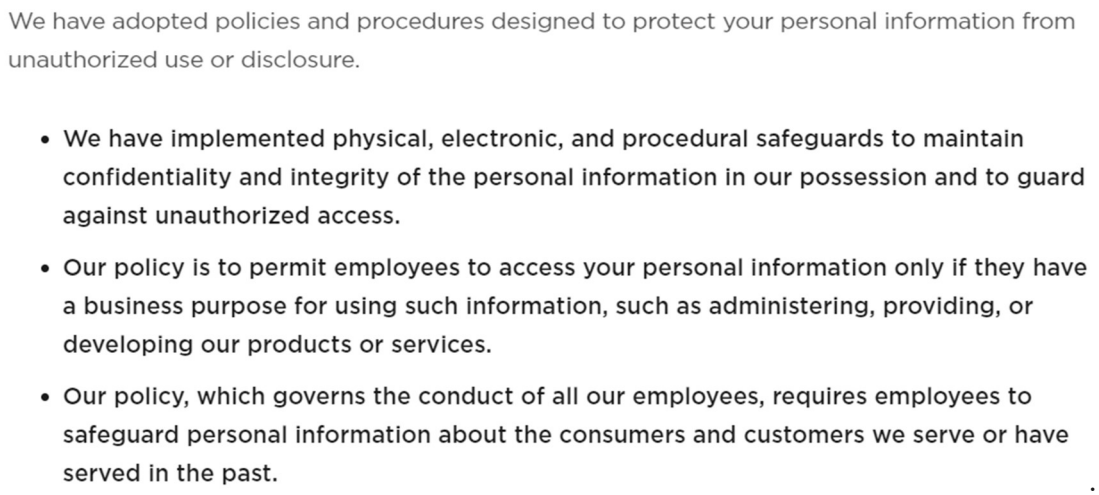
[2] *Id.*



Our Privacy Pledge

- **We do not sell or rent customer information. Period.**
- We share customer information with certain employees and with companies providing services on our behalf to service your needs.
- We may share your personal information with non-affiliates to assist in your application and mortgage process.
- We may share information for marketing and/or joint marketing purposes.
- Our policy requires all employees and companies providing services on our behalf to keep customer information safe and to comply with our company's customer information security expectations.
- Our privacy policy applies to potential customers as well as current and former customers.
- You may have other privacy protections under applicable state laws. To the extent the state laws apply, we will comply with them when we share information about you, and in some cases may be limited by you in what we can share.

38. Defendant Lower reassures consumers that its policies and procedures will protect consumers' PII from disclosure: [3]



We have adopted policies and procedures designed to protect your personal information from unauthorized use or disclosure.

- We have implemented physical, electronic, and procedural safeguards to maintain confidentiality and integrity of the personal information in our possession and to guard against unauthorized access.
- Our policy is to permit employees to access your personal information only if they have a business purpose for using such information, such as administering, providing, or developing our products or services.
- Our policy, which governs the conduct of all our employees, requires employees to safeguard personal information about the consumers and customers we serve or have served in the past.

Lower Failed to Safeguard Consumers' PII

39. Defendant Lower obtains consumers' PII through mortgage loan applications.

[3] *Id.*

40. On July 28, 2017, Plaintiff Solomon applied for a mortgage with Homeside Financial.

41. Plaintiff Leithren applied for and obtained a mortgage loan with lender, Cenlar, which he paid off in June of 2019.

42. On information and belief, Defendant Lower obtained the PII of the Plaintiffs through those mortgage products or other indirect means and/or sharing with affiliates and/or non-affiliates.

43. Defendant Lower had a duty to keep the PII of the Plaintiffs and Class Members secure.

44. Notwithstanding the duty to keep the PII of the Plaintiffs and Class Members secure, an unauthorized actor accessed the Lower network and removed files from the network between December 10, 2021, and December 14, 2021.

45. Notwithstanding the duty to keep the PII of the Plaintiffs and Class Members secure, an unauthorized actor accessed certain employee email accounts between September 2, 2021 and December 16, 2021.

The Data Breach

46. On April 28, 2022, Defendant discovered that during a review of the 2021 Data Breach that certain personal information, including Plaintiffs' Social Security Numbers and names were viewed and exfiltrated from its system without authorization. Defendant also informed Plaintiffs and Class Members that they also maintain dates of birth, driver's license information, and financial account information and that this too may have been impacted by the Data Breach.

47. According to Defendant, it took unidentified steps to secure its email system, and then allegedly launched an investigation into the matter. Nevertheless, Defendant was unable to

determine the scope of the Data Breach until five months later and attackers had access to employee email accounts for two full days following the breach.

48. To date, Defendant has not revealed most (if not all) of the findings of the investigation it commissioned. Defendant has not revealed the mechanism by which the unauthorized actor first gained access to their systems. Defendant has not revealed the scope or nature of the intrusion into its systems between September and December 2021. Defendant has not revealed whether additional employee email accounts were subsequently breached, or whether the unauthorized actor was able to access Defendant's broader computer systems and network.

49. Even worse, Defendant has failed to disclose the exact nature of the unauthorized access to Plaintiffs' and Class Members' PII. Instead, Defendant speaks in generalities and equivocations, claiming that it only knows that "it is possible [additional information we maintain] may have also been on an involved system," and "the ongoing review of the involved Lower systems identified your name and social security number."

50. This "disclosure" amounts to no real disclosure at all, as it fails to inform Plaintiffs and Class Members what information belonging to them was affected, leaving Plaintiffs and Class Members to believe that all of this incredibly sensitive PII was compromised in this Data Breach.

51. Defendant's offering of credit and identity monitoring establishes that Plaintiffs' and Class Members' sensitive PII was in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

52. The unauthorized actor gained access to Defendant's computer systems well in advance of the December 14, 2021 date that the intrusion was first discovered. As Defendant admits in the "Notice of Data Incident" letter, it eventually detected intrusions into its email system from September 2, 2021 to December 16, 2021, two days after it detected the Data Breach. The

unauthorized actor had unfettered and undetected access to Defendant's networks for a considerable period of time prior to and after Defendant becoming aware of the unauthorized access to its computer systems.

53. The investigation commissioned by Defendant did not conclude until April 28, 2022, and notice was not sent to victims of the data breach until nearly a month after that. Thus, the victims of this Data Breach, including Plaintiffs and Class Members, were not sent notice of this Data Breach until approximately six (6) months after Defendant first knew about this Data Breach.

54. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted PII of Plaintiffs and Class Members, including but not limited to name, Social Security Number, driver's license information, and/or financial account number.

55. On February 24, 2022, Defendant Lower sent a breach notification to the Maine Attorney General which indicated 1,647 people throughout the country had their PII exposed in the Data Breach.

56. On May 27, 2022, however, Defendant Lower sent a supplemental breach notification to the Maine Attorney General which indicated the total number of persons affected was much higher—85,958 individuals.

57. Defendant first notified its impacted consumers of the incident on or around May 27, 2022, sending written notifications to individuals whose personal information was compromised in the Data Breach.

58. In August 2022, Plaintiffs Solomon and Leithren received breach notification letters from Lower.

59. The breach notification letter informed Plaintiffs that on December 14, 2021, Lower identified unusual activity on its network. On December 17, 2021, an investigation determined that

an unauthorized actor accessed the Lower network and removed certain files. The investigation also revealed the unauthorized access to Lower's employee email accounts. Lower competed its review some seven (7) months later – on July 7, 2022.

60. Lower's Breach Notice stated that given the Data Breach, Lower was "reviewing [] existing policies and procedures and implementing additional safeguards to further secure the information in our systems as appropriate."

61. Plaintiffs' and Class Members' PII was accessed and stolen in the Data Breach.

62. Plaintiffs further believe their PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type

63. To prevent and detect cyber-attacks attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

64. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[4]

65. To prevent and detect cyber-attacks attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

[4] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at:* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Nov. 11, 2021).

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[5]

66. Upon information and belief, Defendant also transmitted and stored unencrypted PII in employee emails, a grossly negligent act.

67. Given that Defendant was storing the PII of Plaintiffs and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyber-attacks.

68. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent what appears to be an email phishing attack (which is the most common and easily thwarted form of cyberattack), resulting in the Data Breach and the exposure of the PII of an undisclosed amount of current and former consumers, including Plaintiffs and Class Members.

[5] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Nov. 11, 2021).

69. Defendant could have prevented this Data Breach by instituting policies and practices not to transmit or store unencrypted PII in employee email account, or by properly securing and encrypting the emails, files and file servers containing the PII of Plaintiffs and Class Members.

70. Defendant's negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

71. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

Defendant Knew or Should Have Known of the Risk Because the Financial Services Sector is Particularly Susceptible to Cyber Attacks

72. Defendant knew and understood unprotected or exposed PII in the custody of financial services firms such as Defendant is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access, as mortgage and lending firms maintain highly sensitive PII, including Social Security numbers and financial information.

73. Moreover, it has been well-reported that the banking/credit/financial services industry is one of the most "at-risk" industries when it comes to cybersecurity attacks.[6] Attacks against the financial sector increased 238% globally from the beginning of February 2020 to the end of April, with some 80% of financial institutions reporting an increase in cyberattacks, according to cyber security firm VMware.

Value of Personally Identifiable Information

74. The Federal Trade Commission ("FTC") defines identity theft as "a fraud

[6] *See, e.g.,* https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/financial-services-risk-cyber.html.

committed or attempted using the identifying information of another person without authority."[7] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[8]

75. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained. Other sources note that Personal Information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[9] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[10] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[11]

76. Social Security numbers, for example, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

---

[7] 17 C.F.R. § 248.201 (2013).
[8] *Id*.
[9] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Jan. 19, 2022).
[10] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Jan 19, 2022).
[11] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Jan. 19, 2022).

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[12]

77. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

78. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[13]

79. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license number, addresses, and financial information.

80. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information,

---

[12] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 19, 2022).

[13] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Jan. 19, 2022).

personally identifiable information and Social Security numbers are worth more than 10x on the black market."[14]

81. Among other forms of fraud, identity thieves may use Social Security numbers to obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

82. Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[15]

83. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you.
>
> Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.[16]

84. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless

---

[14] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Nov. 11, 2021).

[15] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last accessed July 20, 2021).

[16] Sue Poremba, *What Should I Do If My Driver's License Number is Stolen?"* (October 24, 2018) https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last accessed July 20, 2021).

piece of information to lose if it happens in isolation."[17] However, this is not the case. As cybersecurity experts point out:

> "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks."[18]

85. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[19]

86. The fraudulent activity resulting from the Data Breach may not come to light for years.

87. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[20]

88. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, including but not limited to name, Social Security Number, driver's license information, and/or financial account information, and of the foreseeable consequences that would occur if Defendant's data security system and

---

[17] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last accessed July 20, 2021).
[18] *Id.*
[19] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021 https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last accessed July 20, 2021).

[20] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Jan. 19, 2022).

network was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

89. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

90. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially thousands of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

91. In the breach notification letter, Defendant made an offer of 12 months of single bureau credit and identity monitoring services. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' PII.

92. Defendant's own notice letter acknowledges the inadequacy of the one year of credit protection it offers because the very next paragraph recommends that affected customers self-monitor their accounts and credit reports for up to two years.

93. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

94. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security

numbers and financial information, fraudulent use of that information and damage to victims may continue for years.

Defendant Violated the Gramm-Leach-Bliley Act

95. Defendant is a financial firm that gives mortgage loans to individuals and businesses, and therefore is subject to the Gramm-Leach-Bliley Act ("GLBA").

96. Defendant collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Defendant was subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1 et seq., and is subject to numerous rules and regulations promulgated on the GLBA Statutes. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the Consumer Financial Protection Bureau ("CFPB") became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

97. Accordingly, Defendant's conduct is governed by the Privacy Rule prior to December 30, 2011, and by Regulation P after that date.

98. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous."16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy

policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Defendant violated the Privacy Rule and Regulation P.

99. Upon information and belief, Defendant failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing and/or sharing that PII on its network. Plaintiffs do not recall receiving any privacy notice from Defendant.

100. Defendant failed to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on its inadequately secured network and would do so after the customer relationship ended.

101. The Safeguards Rule, which implements Section 501(b) of the GLBA,15 U.S.C. § 6801(b), requires institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk

assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein, Defendant violated the Safeguard Rule.

102. Defendant failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of PII in its custody or control.

103. Defendant failed to design and implement information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

104. Defendant failed to adequately oversee service providers.

105. Defendant failed to evaluate and adjust its information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.

Defendant Violated the FTC Act

106. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

107. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein.

Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Nationwide Class.

Plaintiff Dale Foster's Experience

108. Based upon the Notice of Data Incident letter that he received, Plaintiff's PII, including but not limited to his name, Social Security Number, date of birth, driver's license information, and/or financial account information, was acquired, stored, and maintained by Defendant.

109. To date, Defendant has done next to nothing to adequately protect Plaintiff Foster and Class Members, or to compensate them for their injuries sustained in this Data Breach.

110. Defendant's data breach notice letter downplays the theft of Plaintiffs' and Class Members' PII, when the facts demonstrate that the PII was targeted, accessed, and exfiltrated in a criminal cyberattack. The fraud and identity monitoring services offered by Defendant are only for one year and place the burden squarely on Plaintiffs and Class Members by requiring them to expend time signing up for the service and addressing timely issues.

111. Moreover, despite offering only twelve months of credit monitoring, Defendant instructs Plaintiffs and members of the Class to mitigate their damages by self-monitoring their accounts and credit reports for up to two years to ensure that they remain uncompromised as a result of Defendant's failure to properly secure their PII.

112. Plaintiffs and Class Members have been further damaged by the compromise of their PII.

113. Because Plaintiff Foster's PII was exfiltrated by an unauthorized third party it should be assumed that Plaintiff's and each Class Member's PII has been offered for sale on internet forums as that is the *modus operandi* of data thieves.

114. Plaintiff Foster's PII was compromised in the Data Breach and was likely stolen and in the hands of cybercriminals who illegally accessed Defendant's computer systems for the specific purpose of targeting the PII.

115. Plaintiff Foster typically takes measures to protect his PII and is very careful about sharing his PII. Plaintiff Foster has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

116. Plaintiff Foster stores any documents containing his PII in a safe and secure location, and he diligently chooses unique usernames and passwords for his online accounts.

117. As a result of the Data Breach, Plaintiff Foster has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. He has spent at least five hours monitoring his accounts and credit scores, researching Lower LLC, changing the passwords to his accounts and otherwise researching how he has been impacted by the Data Breach. This is time that was lost and unproductive and took away from other activities and duties.

118. Plaintiff Foster also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and as a result of the Data Breach.

119. Plaintiff Foster suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

120. Plaintiff Foster has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his name and Social Security Number being placed in the hands of criminals.

121. Defendant obtained and continues to maintain Plaintiff Foster's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff Foster would not have entrusted his PII to Defendant had he known that it would fail to maintain adequate data security. Plaintiff Foster's PII was compromised and disclosed as a result of the Data Breach.

122. As a result of the Data Breach, Plaintiff Foster anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Foster is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Solomon's Experience

123. As a condition of obtaining her mortgage, Plaintiff Solomon to provide her PII.

124. Lower was entrusted with Plaintiff Solomon's PII and trusted that the company would use reasonable measures to protect it according to Lower's internal policies, public privacy policy, and state and federal law.

125. In November 2021, Plaintiff Solomon had two bank accounts opened in her name (one at Regions Bank and the other at Woodforest National Bank) without her authorization. Upon information and belief, both unauthorized accounts stemmed from Defendant Lower's mishandling of her PII and/or the Data Breach. Plaintiff Solomon used the email realestatedriven@gmail.com to apply for mortgages and both banks notified her of the account openings using that same email address.

126. As a result of the Breach Notice, Plaintiff Solomon spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Breach Notice, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. She also spent time going to the police department and filing a police report, calling both banks multiple times to file a fraud report with each bank and close the accounts (which was not done right away), filing a report with the FLHSMV and flagging her license, freezing her credit, and researching where this breach came from. This time has been lost forever and cannot be recaptured.

127. Plaintiff Solomon has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff Solomon fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff Solomon has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

128. Plaintiff Solomon suffered actual injury in the form of damages to and diminution in the value of Plaintiff Solomon's PII—a form of intangible property that Plaintiff Solomon entrusted to Defendant, which was compromised in and as a result of the Data Breach.

129. Plaintiff Solomon has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties and possibly criminals.

130. Plaintiff Solomon has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Leithren's Experience

131. As of obtaining his mortgage, Plaintiff Leithren it required Plaintiff Leithren to provide his PII.

132. Lower was entrusted with Plaintiff Leithren's PII and he trusted that the company would use reasonable measures to protect it according to Lower's internal policies, public privacy policy, and state and federal law.

133. Plaintiff Leithren believes his name and Social Security number were compromised in the Data Breach.

134. As a result of the Breach Notice, Plaintiff Leithren spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Breach Notice, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

135. Plaintiff Leithren has and will spend considerable time and effort monitoring her accounts to protect himself from additional identity theft. Plaintiff Leithren fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff Leithren has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

136. Plaintiff Leithren suffered actual injury in the form of damages to and diminution in the value of Plaintiff Leithren's PII—a form of intangible property that Plaintiff Leithren entrusted to Defendant, which was compromised in and as a result of the Data Breach.

137. Plaintiff Leithren has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

138. Plaintiff Leithren has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

139. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

140. As a result of Defendant Lower's failure to prevent the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of defendant and is subject to further breaches so long as defendant fails to undertake the appropriate measures to protect the PII in their possession.

141. As shown above, stolen PII is one of the most valuable commodities on the criminal information black market.

142. The value of Plaintiffs' and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

143. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

144. One such example of criminals using PII for profit is the development of "Fullz" packages.

145. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

146. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII

stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

147. Defendant disclosed the PII of Plaintiffs and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiffs and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

148. Defendant's failure to properly notify Plaintiffs and members of the proposed Class of the Data Breach exacerbated Plaintiffs' and members of the proposed Class's injuries by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

149. To date, Defendant Lower has offered Plaintiffs and Class Members only one year of identity and credit monitoring services through Experian IdentityWorks. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII involved here. Moreover, Lower is putting the burden squarely on Plaintiffs and Class Members to enroll in the inadequate monitoring services.

150. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

CLASS ALLEGATIONS

151. Plaintiffs brings this suit on behalf of themselves and a class of similarly situated individuals under Federal Rule of Civil Procedure 23, which is preliminarily defined as:

> **All persons Lower LLC identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

152. In the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Solomon asserts claims on behalf of a separate subclass (the "Florida Subclass"), defined as follows:

> **All individuals residing in Florida whose PII was compromised in the Data Breach described in the Breach Notice.**

153. In the alternative to claims asserted on behalf of the Nationwide Class and Florida Subclass, Plaintiff Leithren asserts claims on behalf of a separate subclass (the "Maryland Subclass"), defined as follows:

> **All individuals residing in Maryland whose PII was compromised in the Data Breach described in the Breach Notice.**

154. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

155. Plaintiffs and the Class Members satisfy the numerosity, commonality, typicality, adequacy, and predominance prerequisites for suing as representative parties Federal Rule of Civil Procedure 23.

156. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, public news reports indicate that approximately 87,605 individuals had their PII compromised in this Data Breach. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

157. **Commonality.** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Plaintiffs and Class Members to safeguard their PII;

f. Whether Defendant breached its duty to Plaintiffs and Class Members to safeguard their PII;

g. Whether computer hackers obtained Plaintiffs' and Class Members' PII in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's conduct was *per se* negligent, and;

l. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

158. **Typicality.** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class member, was compromised in the Data Breach.

159. **Adequacy of Representation.** Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel is competent and experienced in litigating Class actions, including data privacy litigation of this kind.

160. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

161. **Superiority.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

162. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

163. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiffs and the Class, or alternatively the Subclasses)

164. Plaintiffs re-allege and incorporate by reference each of the preceding paragraphs as though fully incorporated herein.

165. Defendant knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and

protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

166. Defendant had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' PII.

167. Defendant Lower owed a duty of care to Plaintiffs and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant Lower acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and members of the Class's PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

168. Defendant Lower owed to Plaintiffs and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

169. Defendant Lower owed these duties to Plaintiffs and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate

security protocols. Defendant Lower actively sought and obtained Plaintiffs' and members of the Class's personal information and PII.

170. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

171. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

172. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had and voluntarily undertook a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

173. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair. . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

174. Defendant's duty to use reasonable security measures also arose under the GLBA, under which Defendant was required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

175. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes), and the GLBA, were intended to protect.

176. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' PII within Defendant's possession.

177. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' and Class Members' PII.

178. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiffs and Class Members that the PII within Defendant's possession might have been compromised and precisely the type of information compromised.

179. Defendant's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' PII to be compromised.

180. As a result of Defendant's ongoing failure to notify Plaintiffs and Class Members regarding the type of PII has been compromised, Plaintiffs and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

181. Defendant's breaches of duty caused Plaintiffs and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their PII.

182. As a result of Defendant's negligence and breach of duties, Plaintiffs and Class Members are in danger of imminent harm in that their PII, which is still in the possession of third parties, will be used for fraudulent purposes.

183. Plaintiffs seek the award of actual damages on behalf of themselves and the Class.

184. In failing to secure Plaintiffs' and Class Members' PII and promptly notifying them of the Data Breach, Defendant is guilty of oppression, fraud, or malice, in that Defendant acted or failed to act with a willful and conscious disregard of Plaintiffs' and Class Members' rights. Plaintiffs, therefore, in addition to seeking actual damages, seek punitive damages on behalf of themselves and the Class.

185. Plaintiffs seek injunctive relief on behalf of the Class in the form of an order compelling Defendant to institute appropriate data collection and safeguarding methods and policies with regard to patient information.

SECOND CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

186. Plaintiffs re-allege and incorporate by reference each of the preceding paragraphs 1 through 163 as though fully incorporated herein.

187. Defendant benefited from receiving Plaintiffs' and Class Members' PII by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

188. Defendant also understood and appreciated that Plaintiffs' and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

189. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of providing (or having third parties provide on their behalf) their PII to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. In exchange, Plaintiffs and Class members should have received adequate protection and data security for such PII held by Defendant.

190. Defendant knew Plaintiffs and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiffs and Class Members for business purposes.

191. Defendant failed to provide reasonable security, safeguards, and protections to the PII of Plaintiffs and Class Members.

192. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

193. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiffs and Class Members.

194. Defendant's enrichment at the expense of Plaintiffs and Class Members is and was unjust.

195. As a result of Defendant's wrongful conduct, as alleged above, Plaintiffs and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

THIRD CAUSE OF ACTION
NEGLIGENCE *PER SE* / VIOLATION OF A STATUTE OR ORDINANCE
(On Behalf of Plaintiffs and the Class, or Alternatively the Subclasses)

196. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 163.

197. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

198. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

199. Defendant's duty to use reasonable security measures also arose under the GLBA, under which Defendant was required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

200. Defendant's violations of Section 5 of the FTC Act and GLBA (and similar state statutes) constitute negligence per se and/or a violation of Maryland's statute or ordinance rule which establishes a *prima facie* case of Defendant's negligence.

201. Defendant's violation of the GLBA and its Safeguards Rule constitutes negligence *per se.*

202. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes), and the GLBA, were intended to protect.

203. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members. The GLBA, with its Safeguards Rule, was similarly intended.

204. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of

identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm entitling them to damages in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
Violation of Maryland's Consumer Protection Act
(On Behalf of Plaintiff Leithren and the Maryland Subclass)

205. Plaintiff Leithren re-alleges and incorporates by reference herein all of the preceding allegations. Plaintiff Leithren brings this Count on his own behalf and that of the Maryland Subclass (the "Class" for the purpose of this Count).

206. The Maryland Consumer Protection Act (hereinafter "MCPA") is expressly intended to protect "consumers" like Plaintiff Leithren and Class Members from unfair or deceptive trade practices.

207. The MCPA, "[s]hall be construed and applied liberally to promote its purpose. It is the intent of the General Assembly that in construing the term "unfair or deceptive trade practices," due consideration and weight be given to the interpretation of § 5 (a)(1) of the Federal Trade Commission Act by the Federal Trade Commission and the federal courts." MD. CODE ANN., COM. LAW § 13-105 (2021).

208. Plaintiff Leithren and Class Members have a vested interest in the privacy, security, and integrity of their PII in connection with Defendant Lower's business, sales, representations and operations as contemplated by the MCPA.

209. Defendant is based in Maryland and is a "person" and/or "merchant" subject to the MCPA.

210. Plaintiff Leithren and Class Members are "consumers" that have been damaged by the Data Breach and exposure of their PII due to Defendant Lower's violations of its own Privacy Policies and Pledges and violations of the FTC Act amongst other deceptive and unfair conduct.

211. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of MCPA, including: (1) failing to maintain adequate data security to keep Plaintiff's and the Class's sensitive PII from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (2) failing to disclose or omitting materials facts to Plaintiff Leithren and the Class regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the PII of Plaintiff Leithren and the Class; (3) failing to disclose or omitting materials facts to Plaintiff Leithren and the Class about Defendant's failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII of Plaintiff Leithren and the Class; and (4) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff Leithren and the Class's PII and other personal information from further unauthorized disclosure, release, data breaches, and theft.

212. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about its inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff Leithren and the Class and defeat their reasonable expectations about the security of their PII.

213. Defendant intended that Plaintiff Leithren and the Class rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services including but not limited to Defendant Lower's Privacy Policies and Pledges.

214. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Class. Plaintiff the Class have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

215. Defendant also violated MCPA by failing to immediately notify Plaintiff Leithren and the entire Class of the nature and extent of the Data Breach pursuant to MD. CODE ANN., COM. LAW § 14-3501 et. seq. which requires notification within 45 days.

216. As a result of Defendant Lower's wrongful conduct, Plaintiff Leithren and the Class were injured in that they never would have permitted Defendant to obtain their PII had they known or been told that Defendant failed to maintain sufficient security to keep their PII from being hacked and taken and misused by others.

217. As a direct and proximate result of Defendant's violations of MCPA, Plaintiff Leithren and the Class have suffered harm, including possible instances of identity theft; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against

future identity theft; lost control over the value of their PII; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

218. Plaintiff Leithren and Class Members have suffered ascertainable losses as a direct result of Defendant's employment of unconscionable acts or practices, and unfair or deceptive acts or practices.

219. Plaintiff Leithren and the Class are entitled to an award of attorneys' fees, costs and other recoverable expenses of litigation.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and on behalf of Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiffs and their Counsel to represent each such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised,

hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Dated: September 6, 2022

Respectfully, submitted,

By: */s/ Thomas Pacheco*

Thomas Pacheco (Bar No. 21639)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
15453 Indianola Drive
Derwood, MD 20855
Telephone: (443) 980-6119
tpacheco@milberg.com

David Lietz (admitted *pro hac vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Ave. NW, Suite 440
Washington DC 20015
Phone: (866) 252-0878
Fax: 202-686-2877
dlietz@milberg.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Samuel J. Strauss*
Raina C. Borrelli*
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
T: (608) 237-1775
F: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

(* *pro hac vice* forthcoming)

Attorneys for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on September 6, 2022 the foregoing document was filed via the Court's ECF system, which will cause a true and correct copy of the same to be served electronically on all ECF-registered counsel of record.

/s/ Thomas Pacheco
Thomas Pacheco